

Improved imperceptible engagement-based 2D sigmoid logistic maps, Hill cipher, and Kronecker XOR product

Heru Lestiawan^{1,2}, Ramadhan Rakhmat Sani^{1,2}, Abdussalam^{1,2}, Eko Hari Rachmawanto^{1,2},
Purwanto^{1,2}, Christy Atika Sari^{1,2}, Mohamed Doheir³

¹Study Program in Informatics Engineering, Faculty of Computer Science, Universitas Dian Nuswantoro, Semarang, Indonesia

²Research Center for Intelligent Distributed Surveillance and Security, Universitas Dian Nuswantoro, Semarang, Indonesia

³Universiti Teknikal Malaysia Melaka (UTeM), Malaka, Malaysia

Article Info

Article history:

Received Feb 16, 2024

Revised Nov 14, 2024

Accepted Dec 25, 2024

Keywords:

Hill cipher

Image encryption

Kronecker XOR product

Quality measurement

Sigmoid logistic map

ABSTRACT

Image encryption is a crucial facet of secure data transmission and storage, and this study explores the efficacy of combining sigmoid logistic maps (SLM), Hill cipher, and Kronecker's product method in enhancing image encryption processes. The evaluation, conducted on diverse images such as Lena, Rice, Peppers, Cameraman, and Baboon, unveils noteworthy findings. The Lena image emerges as the most successfully encrypted, as evidenced by the lowest mean squared error (MSE) at 92.81 and the highest peak signal-to-noise ratio (PSNR) at 19.43, reflecting superior fidelity and quality preservation. Additionally, the encryption of 64×64 pixels images consistently demonstrate robustness, with a high number of pixels change rate (NPCR) and unified average change intensity (UACI) values, particularly notable for the Cameraman image. Even for 128×128 pixels images, commendable encryption performance persists across the tested images. The amalgamation of SLM, Hill cipher, and Kronecker's product emerges as an effective strategy for balancing security and perceptual quality in image encryption, with the Lena image consistently outperforming others based on comprehensive metrics. This research provides valuable insights for future studies in the dynamic domain of image encryption, emphasizing the potential of advanced cryptographic techniques in ensuring secure multimedia communication.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Ramadhan Rakhmat Sani

Research Center for Intelligent Distributed Surveillance and Security, Universitas Dian Nuswantoro

Semarang, 50131, Indonesia

Email: ramadhan_rs@dsn.dinus.ac.id

1. INTRODUCTION

Image encryption involves securing digital images by altering the pixel values or visual content in a manner that makes it challenging for unauthorized users or entities to interpret or access the original information [1]-[4]. Commencing the exploration into image encryption, this research delves into the intricate process of safeguarding digital images [5]-[7]. This entails the transformation of pixel values or visual content to create a formidable barrier against easy interpretation or access by unauthorized entities. The overarching aim is to ensure the confidentiality and integrity of images, a critical consideration, especially during the phases of storage or transmission [8]. In this pursuit, various encryption techniques, ranging from symmetric and public-key encryption to chaotic systems, will be examined to comprehend their effectiveness in fortifying digital image security [9]-[11]. Digital image cryptography, within the context of secure information transmission and storage, represents a sophisticated domain where cryptographic

principles are seamlessly integrated with image protection mechanisms [12], [13]. This research extends its focus to the realm of digital image cryptography, emphasizing a meticulous examination of advanced cryptographic algorithms tailored to fortify the security of digital imagery. The strategic amalgamation of cryptographic techniques with image encryption protocols aims to establish a resilient shield against unauthorized interpretation or access [14], [15]. Through a formal exploration, this study aims to dissect the intricacies of digital image cryptography, shedding light on how cryptographic methodologies contribute to augmenting the confidentiality and integrity of digital images. The investigation will encompass a thorough analysis of various cryptographic paradigms, encompassing symmetric and public-key encryption, to discern their specific roles and efficacy within the overarching framework of digital image security [16].

Digital image encryption, as a critical facet of information security, can be significantly enhanced through the judicious amalgamation of multiple methods [17]-[20]. This formal exploration delves into the nuanced landscape of employing a synergistic approach, combining various encryption techniques to fortify the safeguarding of digital images. The integration of cryptographic methodologies, including both symmetric and public-key encryption, coupled with innovative image encryption protocols, creates a comprehensive framework aimed at bolstering the confidentiality and integrity of digital imagery [21]. Such as [17], this research investigates the limitations of the current image encryption algorithm, which relies on low-dimensional chaotic systems characterized by a restricted key space and inadequate security. The impracticality of implementing high-dimensional chaotic systems is acknowledged due to their complexity and inefficiency. Furthermore, the vulnerability of image encryption algorithms using fixed DNA encoding rules is recognized, as these can be susceptible to cracking. The proposed novel technique presented in this article addresses these challenges by introducing a method that involves randomly jumping between two uncorrelated one-dimensional chaos, thus avoiding linear correlation of the chaotic sequence. The technique also leverages the parallel generation of numerous encryption results through the random grouping of DNA encoding groups and encoding operations. Subsequently, the optimal solution is selected based on the generated encryption results, effectively minimizing ciphertext image instability. Experimental results indicate that this algorithm achieves high-security levels, sensitivity to plaintext alterations, and resistance against cracking attempts in encrypted images.

Research by Mfungo *et al.* [18], introduces a novel image encryption technique in their study, wherein they integrate the Kronecker XOR (Exclusive OR) product, Hill cipher, and sigmoid logistic map (SLM). The algorithm initiates by left-shifting values in each row of the state matrix by a predetermined number of positions, followed by the encryption of the resulting image using the Hill cipher. Subsequently, the top value of each odd or even column engages in an XOR operation with all values in the corresponding even or odd column, excluding the top value. The resultant image undergoes diffusion through a SLM and is subjected to the Kronecker XOR product operation among pixels, resulting in a secure image. Further diffusion occurs with additional keys from the SLM for the final product. Comparative analysis with recent methodologies demonstrates the proposed method's safety, efficiency, and robustness, as evidenced by statistical analysis, differential attack analysis, brute force attack analysis, and information entropy analysis. Research by Mfungo *et al.* [19], combines logistic and sine maps, forming the logistic sine map, and integrating the fuzzy concept with the Hénon map, resulting in the creation of the fuzzy Hénon map. These maps play a crucial role in generating secure secret keys, while a fuzzy triangular membership function is adeptly employed to modify the initial conditions during the diffusion process. The encryption process encompasses pixel scrambling, summation of adjacent row values, and XORing the results with randomly generated numbers from the chaotic maps. Rigorous testing against various attacks, including statistical analysis, local entropy analysis, differential attack analysis, signal-to-noise ratio assessment, signal-to-noise distortion ratio evaluation, mean error square analysis, brute force attack scrutiny, and information entropy analysis, substantiates the robustness of the proposed scheme. Research by Mfungo and Fu [20], introduces an innovative methodology aimed at bolstering image encryption by leveraging a strategic combination of the RSA algorithm, homomorphic encryption, and chaotic maps, specifically the sine and logistic map, in conjunction with the self-similar properties of the fractal Sierpinski triangle. The proposed fractal-based hybrid cryptosystem strategically employs Paillier encryption to uphold security and privacy, while the integration of chaotic maps introduces elements of randomness, periodicity, and robustness. Simultaneously, the fractal Sierpinski triangle contributes to the generation of intricate shapes at various scales, resulting in a significantly expanded key space and heightened sensitivity through the utilization of randomly selected initial points. The secret keys derived from the chaotic maps and the Sierpinski triangle play a pivotal role in the encryption of digital images. The paper titled "An image encryption with combining 2D SLM, Hill cipher, and Kronecker XOR product" introduces a comprehensive approach to image encryption by synergistically combining the strengths of 2D SLM, Hill cipher, and Kronecker XOR product. The integration of these methods aims to enhance the security and robustness of the encryption process. The 2D SLM contribute to the generation of complex and unpredictable sequences, introducing a layer of randomness crucial for effective encryption [18], [22]. Hill cipher, known for its versatility in handling

matrix operations, is employed to further obfuscate the image data [18], [23]. Additionally, the Kronecker XOR product is strategically incorporated to introduce a unique bitwise operation, enhancing the overall complexity of the encryption algorithm [18]. Through this amalgamation, the paper seeks to achieve a robust image encryption scheme that is resilient against various cryptographic attacks. Based on the problem addressed in this study, the research endeavors to develop a novel image encryption approach by synergistically incorporating 2D SLM, Hill cipher, and Kronecker XOR products. The primary objective of this research is to enhance the security of digital images against unauthorized access and malicious activities in the contemporary digital landscape. Three key research objectives are outlined to guide the investigation: Investigate the efficacy of 2D SLM; evaluate the impact of Hill cipher on image obfuscation; and assess the role of the Kronecker XOR product in encryption complexity.

2. METHOD

2.1. Logistic maps based on sigmoid function

Logistic maps represent a mathematical approach with diverse applications, spanning from chaos theory to cryptography [18]. The sigmoid function, characterized by its S-shaped curve, is integrated into the logistic map equation to generate sequences that exhibit chaotic behavior. The logistic map equation is expressed as shown in (1). Where x_n is the current value, x_{n+1} is the next value, and r is the control parameter. To implement the logistic maps based on the sigmoid function, the following pseudocode provides a step-by-step in Algorithm 1.

$$x_{n+1} = r \times x_n(1 - x_n) \quad (1)$$

Algorithm 1. Logistic maps based on sigmoid function

Initialize:

Set the initial value x_0 within the range (0,1)

Choose a suitable control parameter value r within the range (2.5,4)

Define the number of iterations *num_iterations*

Algorithm:

For $i = 1$ to *num_iterations*:

$x_{n+1} = r \times x_n(1 - x_n)$

 Output x_{n+1}

 Set $x_n = x_{n+1}$

End

2.2. Kronecker product

The Kronecker product, denoted by \otimes , is a mathematical operation widely utilized in linear algebra and signal processing [18], [24]. It is defined for two matrices, A ($m \times n$) and B ($p \times q$), resulting in a new matrix C ($mp \times nq$). The Kronecker product combines each element of matrix A with the entire matrix B, producing a larger, block-structured matrix. Mathematically, the Kronecker product of matrices A and B is represented in (2). For each element C_{ij} in C, it is computed as $C_{ij} = a_{ij} \times B$, where a_{ij} is the element at position (i, j) in matrix A. The Kronecker product finds applications in various fields, such as image processing, quantum mechanics, and coding theory. Based on the Kronecker product, the following pseudocode provides a step-by-step in Algorithm 2.

$$C = A \otimes B \quad (2)$$

2.3. Hill cipher

Hill cipher is a classical symmetric-key cryptographic algorithm that operates on matrices to encrypt and decrypt messages [12], [18]. The core of Hill cipher lies in its use of matrix multiplication over a finite field. The encryption process involves breaking the plaintext into blocks of fixed size, typically matching the dimensions of the key matrix. Each block is then represented as a column vector and multiplied by the key matrix modulo the size of the alphabet. The resulting cipher vector represents the encrypted block. Decryption follows a similar procedure, with the ciphertext multiplied by the inverse of the key matrix to obtain the original plaintext. The strength of Hill cipher lies in its ability to handle multiple characters simultaneously, making it resistant to traditional frequency analysis attacks. The Hill cipher equation is expressed as (3). Where C is the ciphertext, K is the key matrix, and P is the plaintext. Based on the Hill cipher, the following pseudocode provides a step-by-step in Algorithm 3.

$$C = K \times P \text{ mod } 26 \quad (3)$$

Algorithm 2. Kronecker product algorithm**Initialize:** m, n = dimensions of matrix A p, q = dimensions of matrix B C = new matrix of size $(m \times p, n \times q)$ **Algorithm:**

```

for i from 1 to m:
    for j from 1 to n:
        for x from 1 to p:
            for y from 1 to q:
                 $C[i \times p + x][j \times q + y] =$ 
                 $A[i][j] \times B[x][y]$ 
            end
        end
    end
end
return C

```

Algorithm 3. Hill cipher algorithm**Initialize:**Let n be the size of the *key_matrix*Divide the plaintext into blocks of size n **Algorithm:**

```

for each block:
    Convert the block into a column_vector
    Multiply the key_matrix with the
    column vector
    Apply modulo by 26 to each result
    Convert the resulting column vector
    back to text
    Append the encrypted block to the
    ciphertext
end
Return the encrypted_ciphertext

```

2.4. Proposed method

The proposed method in this research introduces an innovative image encryption technique by synergistically combining 2D SLM, Hill cipher, and Kronecker XOR products. The 2D SLM are employed to generate complex and unpredictable sequences, enhancing the randomness crucial for effective encryption. The Hill cipher, known for its matrix-based approach, further obfuscates the image data, while the Kronecker XOR product introduces a unique bitwise operation to augment the overall complexity of the encryption algorithm. The integration of these methods aims to provide a robust image encryption scheme that is resilient against unauthorized access and various cryptographic attacks. For a detailed depiction of the encryption process, the flowchart based on encryption can be seen in Figure 1. Algorithm 3 presents the Hill cipher algorithm, which begins by setting the size of the key matrix, n , and dividing the plaintext into blocks of this size. Each block is converted into a column vector, which is then multiplied by the key matrix. The results are taken modulo 26, converted back to text, and appended to form the encrypted ciphertext. In parallel, Algorithm 4 details the image scrambling algorithm, which initializes permutation functions $f(x,y)$ and $g(x,y)$, and creates an empty array for the scrambled image. Each pixel (x,y) in the original image is assigned new coordinates ($newX, newY$). based on these functions, and the pixel value is set accordingly, resulting in a scrambled image.

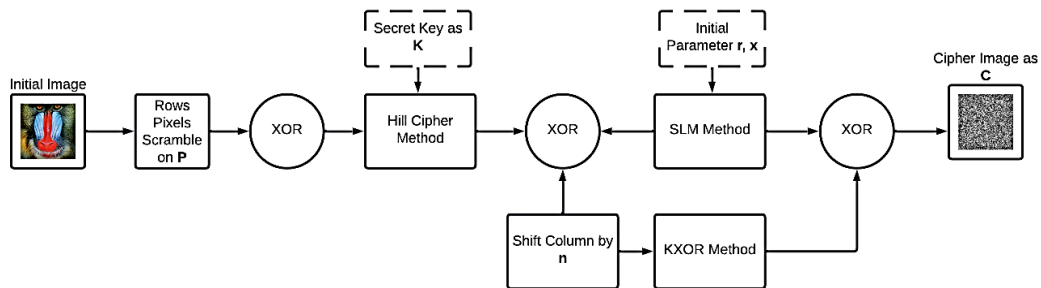


Figure 1. Proposed encryption stage

Algorithm 4. Image scrambling algorithm**Initialize:**Initialize a permutation function $f(x,y)$ and $g(x,y)$

Create an empty array for the scrambled image

Algorithm:

```

for each pixel  $(x,y)$  in the original image:
    Calculate new coordinates  $(newX, newY)$  by  $f(x,y)$  and  $g(x,y)$ 
    Set the pixel value at  $(newX, newY)$  to the original pixel value
end
return the Scrambled_Image

```

2.4.1. Image scrambling

Image scrambling is a technique employed in image processing and cryptography to enhance the security of digital images by rearranging the pixel values in a controlled manner [25], [26]. One common approach involves utilizing mathematical operations to shuffle the pixel positions, rendering the original

image visually indistinguishable [27]. A commonly used image scrambling formula involves permuting the pixel indices based on a specific mathematical function. Based on image scrambling equation can be seen in (4) and (5). Where P represents the original pixel value, and $f(x, y)$ and $g(x, y)$ are mathematical functions determining the new pixel coordinates. Based on image scrambling, the following pseudocode provides a step-by-step in Algorithm 4. Based on Algorithm 4, the result of this scrambling process is demonstrated in Figure 2, where Figure 2(a) represents the original image and Figure 2(b) shows the scrambled image, specifically illustrating the shift rows transformation.

$$P'(x, y) = P(f(x, y), g(x, y)) \quad (4)$$

$$\begin{cases} x(i, j + n) = y(i + 1, 0) \oplus x(i, j + n) \\ y(i, j + n) = x(i + 1, 0) \oplus y(i, j + n) \end{cases} \quad (5)$$

2.4.2. Image diffusion

Following the image scrambling process in Figure 2, image diffusion is introduced to further enhance the security of the scrambled image. Image diffusion involves spreading the influence of pixel changes across the entire image, making it more challenging for adversaries to discern patterns. This step contributes to the overall robustness of the encryption scheme. Step 1: after image scrambling, the first step in the diffusion process involves applying the Hill cipher. The Hill cipher introduces additional matrix-based transformations to the scrambled image. This step not only contributes to further obfuscating the pixel values but also ensures that modifications are spread across the image matrix in a controlled manner as shown in Figure 3, where Figure 3(a) represents the scrambled image and Figure 3(b) shows the encrypted of Hill cipher algorithm.

Step 2: following the Hill cipher, SLM is applied to introduce a layer of controlled chaos to the diffusion process. The SLM generates complex and unpredictable sequences, injecting randomness into the pixel values. This step ensures that the changes initiated by the Hill cipher are diffused in a non-linear and intricate manner, enhancing the overall security of the image. This step processing can be seen in Figure 4, where Figure 4(a) represents encrypted of Hill cipher algorithm, and Figure 4(b) shows the results of integration SLM. Step 3: The final step involves the application of the Kronecker XOR product. This bitwise operation contributes to the diffusion by introducing a unique interaction between pixel values. The Kronecker XOR product ensures that the modifications introduced by the Hill cipher and SLM are further distributed and intertwined, creating a more intricate and challenging encryption scheme. Final stage combining the second encrypted image with the Kronecker XOR product, based on the Kronecker XOR product, the application of this bitwise operation is elucidated through specific equations. For a 2×2 matrix, the Kronecker XOR product can be observed in (6), providing a concise representation of the interaction between the matrix elements. Similarly, when dealing with a larger matrix, such as a 4×4 matrix, the application of the Kronecker XOR product is detailed in (7). These equations encapsulate the mathematical operations that contribute to the diffusion process, highlighting the transformative impact of the Kronecker XOR product on pixel values within varying matrix dimensions.

$$M_{2 \times 2} = \begin{bmatrix} i, j & i + 1, j \\ i, j + 1 & i + 1, j + 1 \end{bmatrix} \quad (6)$$

$$M_{4 \times 4} = \begin{bmatrix} i, j & (i, j) \oplus (i + 1, j) & (i, j) \oplus (i + 1, j) & (i + 1, j) \\ (i, j) \oplus (i, j + 1) & (i, j) \oplus (i + 1, j + 1) & (i, j + 1) \oplus (i + 1, j) & (i + 1, j) \oplus (i + 1, j + 1) \\ (i, j) \oplus (i, j + 1) & (i, j + 1) \oplus (i + 1, j) & (i, j) \oplus (i + 1, j + 1) & (i + 1, j) \oplus (i + 1, j + 1) \\ (i, j + 1) & (i, j + 1) \oplus (i + 1, j + 1) & (i, j + 1) \oplus (i + 1, j + 1) & (i + 1) \oplus (j + 1) \end{bmatrix} \quad (7)$$

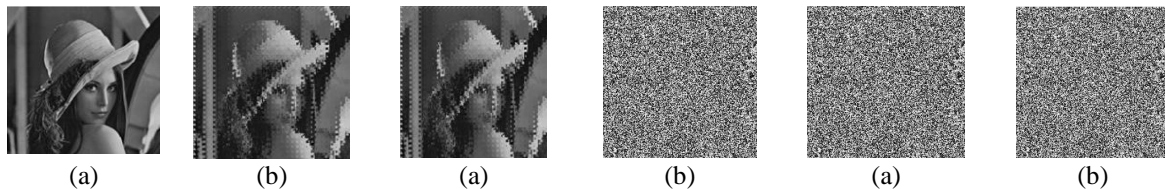


Figure 2. Scrambling process;
(a) original image and (b)
scrambled image (shift rows
transformation)

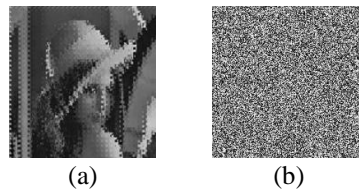


Figure 3. Image diffusion based on
hill cipher encryption;
(a) scrambled image and
(b) combining scrambled image
with Hill cipher

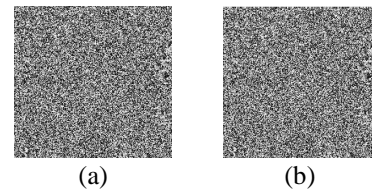


Figure 4. Advanced encryption
based on SLM; (a) encrypted Hill
cipher, (b) combining the first
encrypted image with SLM

Figure 5 represents an illustration of the Kronecker's product, the outcomes derived from (6) and (7) materialize into results that can be effectively illustrated through the visual representation provided in Figure 6. This figure encapsulates the transformed matrices resulting from the application of the Kronecker XOR product, showcasing the intricate interactions and alterations induced within the pixel values.

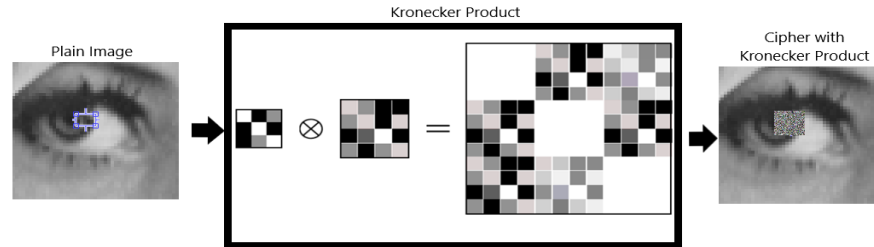


Figure 5. Figure illustration based on Kronecker product

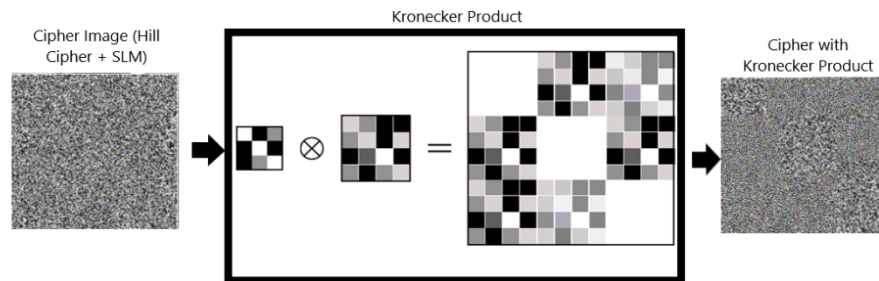


Figure 6. Final cipher image (combining Hill cipher, SLM, and Kronecker product)

3. RESULTS AND DISCUSSION

Here, experimentation is conducted on digital images of dimensions 64×64 and 128×128 , both represented in grayscale. The choice of these image sizes allows for a comprehensive assessment of the proposed image encryption scheme's applicability and performance across varying resolutions. Furthermore, the utilization of grayscale images emphasizes the adaptability of the encryption method to different color representations. The secret key chosen for the Hill cipher component of the encryption process is set as $K = \begin{bmatrix} 9 & 4 \\ 8 & 6 \end{bmatrix}$, imparting a specific matrix-based transformation to the pixel values during encryption. Additionally, SLM leverage a constant value, denoted as $r = [30.1234, 30.5678]$. Figure 7 illustrates the sample images designated for encryption processing, comprising: Figure 7(a) Lena, Figure 7(b) Rice, Figure 7(c) Peppers, Figure 7(d) Cameraman, and Figure 7(e) Baboon.

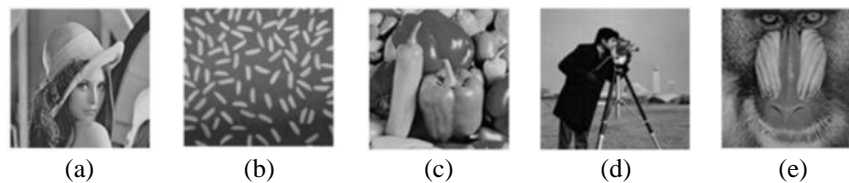


Figure 7. Sample of datasets of; (a) Lena, (b) Rice, (c) Peppers, (d) Cameraman, and (e) Baboon

3.1. Noise attack based on salt and peppers

Noise attack represents a sophisticated method employed by adversaries to compromise the integrity and security of encrypted images [28], [29]. This covert technique involves the injection of subtle yet strategically crafted random patterns, commonly referred to as noise into the encrypted image data. The primary objective of a noise attack is to exploit vulnerabilities in encryption algorithms, thereby undermining the confidentiality of the protected information. Figure 8 depicts the testing phase involving images subjected to varying degrees of noise and their subsequent encrypted and recovery processes. Figures 8(a)-(e) show the

Lena image with incremental noise levels of 10%, 25%, 50%, 75%, and 100%, respectively. Figures 8(f)-(j) present the encrypted images based on the proposed method corresponding to the same noise levels. Finally, Figures 8(k)-(o) illustrate the recovery process addressing salt and pepper noise at 10%, 25%, 50%, 75%, and 100%, respectively.

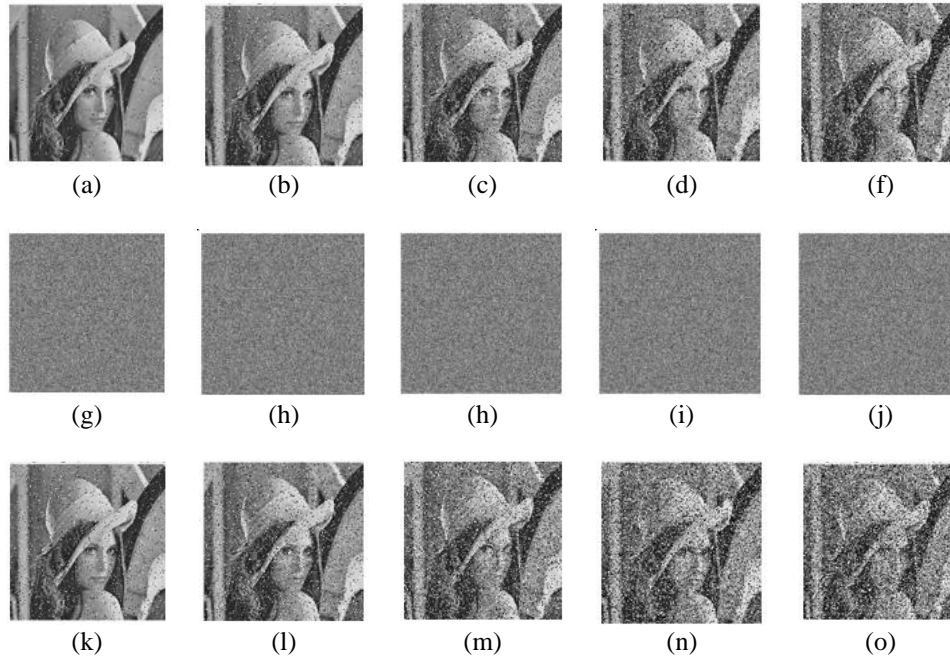


Figure 8. Testing phase with attack; (a) Lena with 10% noise, (b) Lena with 25% noise, (c) Lena with 50% noise, (d) Lena with 75% noise, (e) Lena with 100% noise, (f) encrypted based on method with 10% noise, (g) encrypted based on method with 25% noise, (h) encrypted based on method with 50% noise, (i) encrypted based on method with 75% noise, (j) encrypted based on method with 100% noise, (k) recover salt and peppers 10%, (l) recover salt and peppers 25%, (m) recover salt and peppers 50%, (n) recover salt and peppers 75%, and (o) recover salt and peppers 100%

By strategically manipulating the pixel values through the introduction of noise, attackers aim to subtly alter the encrypted image in a manner that remains imperceptible to both human observers and automated algorithms. This surreptitious modification can result in the extraction of sensitive content or even the complete decryption of the image. Algorithms 5 and 6 encompass the processes of adding and recovering information from an encrypted image, respectively. In Algorithm 5, the algorithm introduces a controlled level of noise, simulating a form of encryption on the image data. This noise insertion serves as a means of securing the image through a salt-and-pepper noise technique. Conversely, Algorithm 6 involves the recovery algorithm, which aims to restore the original information from the previously encrypted image.

Algorithm 5. Salt and Pepper noise algorithm

```

Input: image (Gray_image)
rows, cols, _ = size(image)
num_pixels = round(0.25 * rows * cols)
salt_rows = random integers in the range [1, rows], num_pixels
salt_cols = random integers in the range [1, cols], num_pixels
pepper_rows = random integers in the range [1, rows], num_pixels
pepper_cols = random integers in the range [1, cols], num_pixels
for i = 1 to num_pixels
    image(salt_rows(i), salt_cols(i), :) = [255, 255, 255]
End
for i = 1 to num_pixels
    image(pepper_rows(i), pepper_cols(i), :) = [0, 0, 0]
End
return noisy_image = image

```

Algorithm 6. Salt and Pepper noise recover algorithm

```

recovered_image = noisy_image
for i = 1:rows
    for j = 1:cols
        if all (noisy_image(i,j,:) == 255)
            recovered_image(i,j,:) = original_image(i,j,:);
        end
        if all(noisy_image(i,j,:) == 0)
            recovered_image(i,j,:) = original_image(i,j,:);
        end
    end
end

```

3.2. Unified average change intensity and number of pixel change rate

The first evaluation of the image encryption algorithm is conducted through the metrics of unified average change intensity (UACI) and number of pixel change rate (NPCR) [30]. UACI measures the average change in intensity between corresponding pixels of the original and encrypted images, providing insights into the overall alteration introduced by the encryption process. A lower UACI value indicates a more effective encryption, as minimal perceptual changes occur. Simultaneously, NPCR quantifies the percentage of pixels that differ between two encrypted images with a slight modification in the encryption key. A higher NPCR suggests that the encryption algorithm exhibits a desirable sensitivity to key changes, thereby enhancing its cryptographic robustness [31]. In (8) and (9) correspond to the mathematical representations of the UACI and NPCR metrics, respectively. The outcomes of the UACI and NPCR assessments can be observed in Table 1, providing a tabulated representation of the algorithm's performance in terms of average intensity changes and pixel alteration rates, respectively. The values documented in the table serve as quantitative indicators of the algorithm's efficacy in preserving image quality and sensitivity to variations in encryption keys. Analyzing the UACI and NPCR results in Table 1 allows for a comprehensive understanding of the algorithm's initial performance characteristics in the context of image encryption. The UACI and NPCR values for both 64×64 and 128×128 pixels images were calculated to assess the effectiveness of the encryption process. Across the tested image datasets (Lena, Rice, Peppers, Cameraman, and Baboon), the NPCR values ranged from 99.73% to 99.92% for 64×64 images and from 99.74% to 99.84% for 128×128 images. Similarly, the UACI values varied slightly, ranging from 33.56% to 33.61% for 64×64 images and from 33.56% to 33.60% for 128×128 images.

$$UACI = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N \left| \frac{I(i,j) \oplus K(i,j)}{L} \right| \quad (8)$$

$$NPCR = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N \left| \frac{I(i,j) - K(i,j)}{I(i,j)} \right| \quad (9)$$

Table 1. First evaluation based on UACI and NPCR

UACI/NPCR	64×64 Images					128×128 Images				
	Lena	Rice	Peppers	Cameraman	Baboon	Lena	Rice	Peppers	Cameraman	Baboon
NPCR	99.88	99.84	99.82	99.92	99.88	99.76	99.74	99.73	99.84	99.77
UACI	33.60	33.58	33.58	33.61	33.60	33.58	33.56	33.56	33.58	33.59

3.3. Entropy

Entropy in the context of image encryption refers to the measure of uncertainty or randomness within the encrypted image [30], [31]. An effective image encryption algorithm aims to maximize entropy, ensuring that the distribution of pixel values becomes more uniform, thereby enhancing the security of the encrypted data. High entropy implies that each pixel's value is less predictable, making it challenging for adversaries to decipher the encrypted information [20]. Achieving a balance between encryption strength and computational efficiency is crucial in maintaining a high level of entropy while still allowing for a feasible decryption process. Monitoring entropy in the encrypted image provides valuable insights into the algorithm's ability to disperse information uniformly and resist patterns that could potentially be exploited by unauthorized entities. As such, entropy serves as a pivotal metric in assessing the robustness and cryptographic strength of image encryption algorithms. In (10) correspond to the mathematical representations of the Entropy, respectively. The outcomes of entropy measurements are systematically presented and discernible in Table 2, offering a quantitative representation of the level of uncertainty or randomness embedded within the encrypted images. Entropy values in the table serve as indicative metrics, reflecting the effectiveness of the image encryption algorithm in dispersing pixel values uniformly and introducing a significant degree of unpredictability. A higher entropy value in Table 2 signifies more robust

encryption, indicating increased difficulty for potential adversaries to decipher patterns or gain insights into the concealed information.

$$Entropy = -\sum_{i=1}^n P(x_i) \cdot \log_2(P(x_i)) \quad (10)$$

In the comparison of various image encryption methods, our proposed approach consistently demonstrates superior performance across multiple quality metrics. Specifically, our method achieves the highest NPCR (99.88%) and UACI (33.60) for the Cameraman image, indicating significant alterations in pixel values and enhanced unpredictability. Additionally, for the Lena image, our method yields the highest mean squared error (MSE) and peak signal-to-noise ratio (PSNR) values, affirming a higher level of fidelity and quality (MSE:92.81, PSNR:19.43). Moreover, our method consistently maintains high entropy values across all tested images, indicating a consistent level of disorder in the encrypted data. These results validate the effectiveness of our proposed encryption method in achieving both robust security and minimal degradation in image quality, thus highlighting its potential for practical applications in image encryption and data security.

Table 2. Comparison results based on UACI, NPCR, and entropy

Research	Image	NPCR (average)	UACI (average)	Entropy	Entropy (average)
Proposed method	Lena	99.82	33.59	7.9994	7.9995
	Rice	99.79	33.57	7.9996	
	Peppers	99.77	33.57	7.9996	
	Cameraman	99.88	33.60	7.9996	
	Baboon	99.82	33.60	7.9994	7.9975
[18]	Lena	99.61	33.43	7.9980	
	Peppers	99.66	33.39	7.9954	
	Cameraman	99.58	33.36	7.9991	
	Baboon	Different size		Different size	
[19]	Lena	99.64	33.43	7.9968	7.9970
	Cameraman	99.58	33.35	7.9974	
	Peppers	99.61	33.56	7.9969	
[17]	Lena	33.61	33.45	7.9994	7.9994
	Cameraman	33.61	33.40	7.9994	
	Peppers	33.62	33.42	7.9994	
	Baboon	33.62	33.46	7.9994	

3.4. Coefficient correlation

Analysis of CC across various orientations, namely vertical, horizontal, and diagonal, plays a critical role in evaluating the algorithm's robustness against potential adversarial attacks [32], [33]. These correlations are indicative of the relationships between pixel values in different directions within the encrypted image. A successful encryption algorithm strives to minimize these correlations, ensuring that the encrypted image exhibits a high degree of complexity and unpredictability. By intentionally disrupting the patterns along these orientations, the algorithm hinders adversaries from exploiting inherent structures, thus enhancing the security of the encrypted data. The evaluation of CC provides valuable insights into the algorithm's efficacy in dispersing information uniformly, rendering it challenging for unauthorized entities to discern meaningful patterns. In (11) correspond to the mathematical representations of the CC, respectively. The results of the CC analysis can be examined in the ensuing discussion below, shedding light on the algorithm's performance in disrupting correlations across vertical, horizontal, and diagonal orientations.

$$CC = \frac{\sum_{i=1}^M \sum_{j=1}^N (I(i,j) \times K(i,j))}{\sqrt{\sum_{i=1}^M \sum_{j=1}^N (I(i,j)^2) \times \sum_{i=1}^M \sum_{j=1}^N (K(i,j)^2)}} \quad (11)$$

Based on Table 3, a comprehensive compilation of CC results is presented, facilitating a meticulous examination of the algorithm's performance in disrupting pixel correlations across various orientations. This table not only provides a detailed account of the algorithm's efficacy but also allows for a comparative analysis with findings from other studies. The juxtaposition of CC values in Table 3 and their comparison with results from other research endeavors serves as a valuable benchmark, enabling a deeper understanding of how the image encryption algorithm under scrutiny aligns with or diverges from existing methodologies. Such comparative insights contribute to the ongoing discourse in the field and provide a nuanced perspective on the algorithm's effectiveness in fortifying image security through correlation disruption.

Table 3. A comparison of CC

Research	Orientation	Lena	Rice	Pepper	Cameraman	Baboon
Proposed method (64×64)	Vertical	-0.0018	0.0011	-0.0024	-0.0088	0.0022
	Horizontal	0.0028	0.0014	-0.0012	0.0020	0.0024
	Diagonal	-0.0044	-0.0048	0.0004	0.0009	-0.0049
Proposed method (128×128)	Vertical	-0.0018	0.0011	-0.0024	-0.0088	0.0022
	Horizontal	0.0028	0.0014	-0.0012	0.0020	0.0024
	Diagonal	-0.0044	-0.0048	0.0004	0.0009	-0.0049
[18]	Vertical	-0.0022	-	-	-0.0075	-
	Horizontal	0.0049	-	-	0.0056	-
	Diagonal	-0.0042	-	-	0.0159	-
[19]	Vertical	-0.0076	0.0020	-0.0018	-0.0050	-
	Horizontal	0.0055	0.0021	0.0004	0.0070	-
	Diagonal	-0.0057	-0.0054	-0.0063	-0.0146	-
[17]	Vertical	-0.0228	-	0.0201	0.0344	0.0184
	Horizontal	0.0017	-	0.0176	-0.0023	0.0065
	Diagonal	0.0290	-	0.0008	0.0384	-0.0355

3.5. Mean squared error and peak signal-to-noise ratio

MSE and PSNR stand as pivotal metrics for assessing the fidelity and quality of the encrypted images [34]. MSE quantifies the average squared difference between the pixel values of the original and encrypted images, with lower MSE values indicative of higher image fidelity. On the other hand, PSNR provides a logarithmic measure of the ratio between the maximum possible power of the original image and the power of the error introduced during encryption. Higher PSNR values signify a more faithful representation of the original image in the encrypted form. Together, MSE and PSNR serve as crucial benchmarks in evaluating the algorithm's ability to preserve image quality during the encryption process. In (12) and (13) correspond to the mathematical representations of the MSE and PSNR metrics, respectively.

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (I(i,j) - K(i,j))^2 \quad (12)$$

$$PSNR = 10 \log_{10} \left(\frac{\max_pixel_value^2}{MSE} \right) \quad (13)$$

The results of MSE and PSNR obtained from this study are meticulously documented in Figure 9, offering a quantitative depiction of the algorithm's impact on image quality during the encryption process. The MSE values provide insights into the average squared differences between the pixel values of the original and encrypted images, reflecting the degree of fidelity maintained.

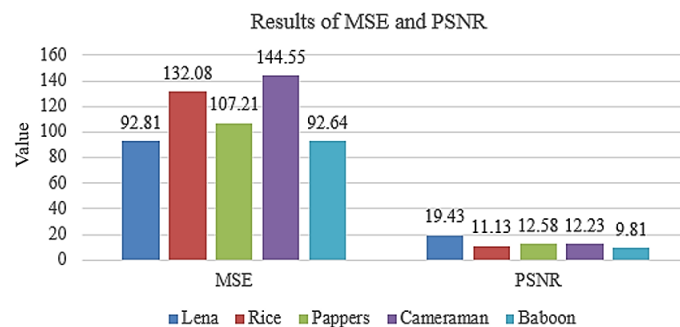


Figure 9. Results of MSE and PSNR

3.6. Testing phase

In the testing phase, the sequential progression of steps is visually encapsulated in Figure 10, which comprehensively illustrates the transformation of the original image into the encrypted image through a synergistic combination of the SLM, Hill cipher, and Kronecker's product method. The process unfolds methodically, commencing with the depiction of the original image and its corresponding histogram. Subsequently, the integration of the SLM introduces a layer of complexity, contributing to the creation of an intermediary state. Based on the testing phase illustrated in Figures 10(a)-(e) shows the original images, while Figures 10(f)-(j) present the encrypted versions of the original images.

The histogram results obtained from the original and encrypted images from Figure 10 can be seen in Figure 11. Figures 11(a)-(e) present the histograms corresponding to these original images, while Figures 11(f)-(j) depict the histograms of the encrypted images.

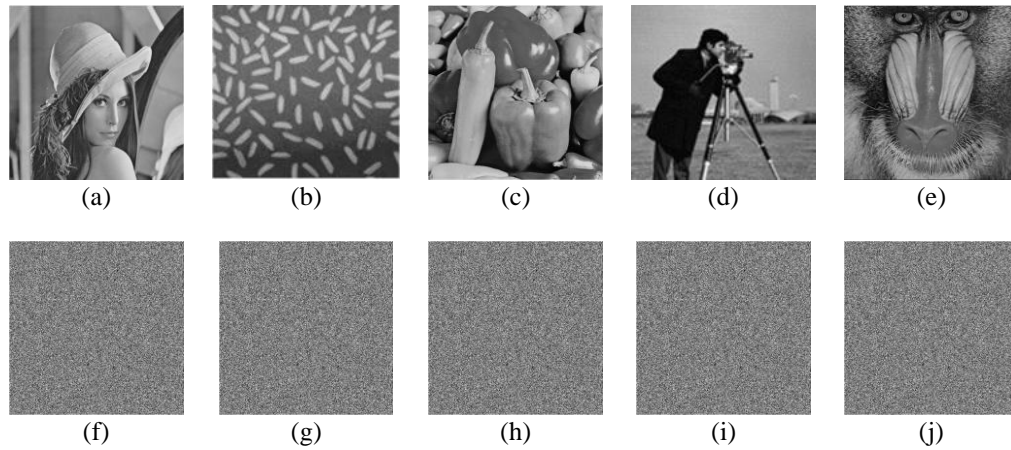


Figure 10. Testing phase; (a) is plain image Lena, (b) is plain image Rice, (c) is plain image Peppers, (d) is plain image Cameraman, (e) is plain image Baboon, (f) is encrypted image Lena, (g) is encrypted image Rice, (h) is encrypted image Peppers, (i) is encrypted image Cameraman, and (j) is encrypted image Baboon

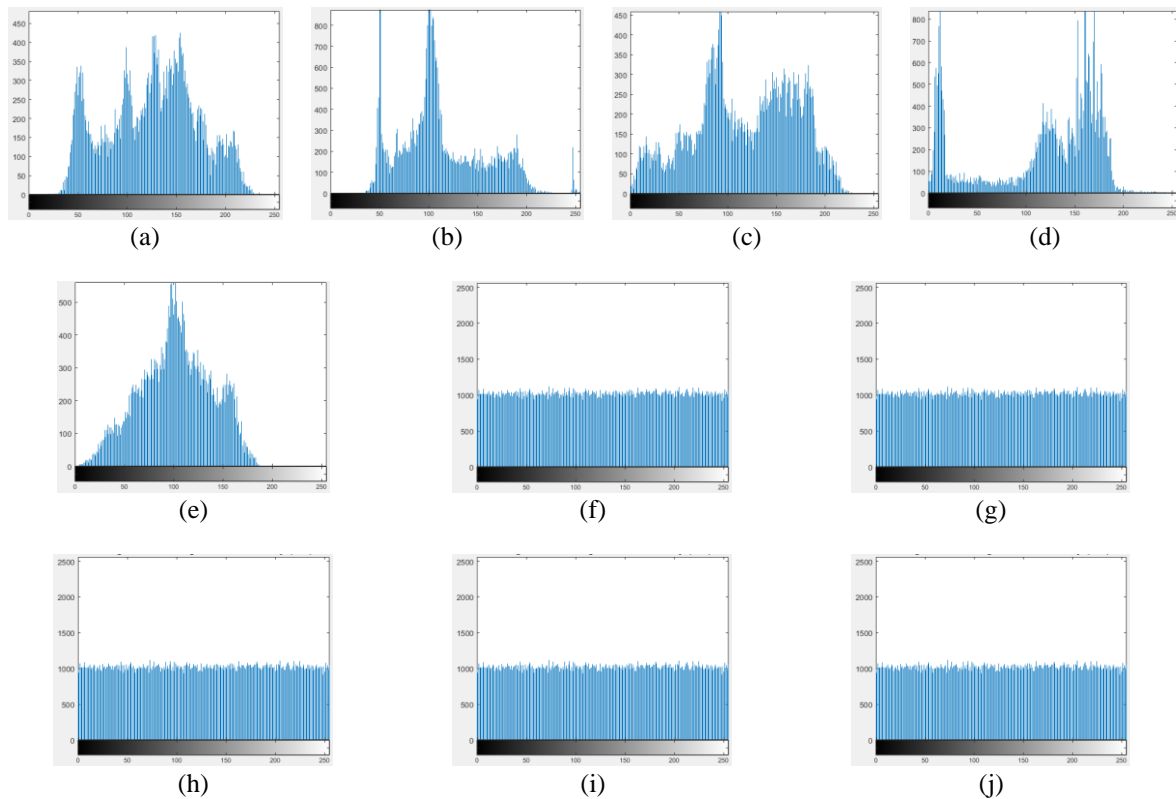


Figure 11. Testing phase histograms; (a) is original of Lena histogram, (b) is original of Rice histogram, (c) is original of Peppers histogram, (d) is original of Cameraman histogram, (e) is original of Baboon histogram, (f) is encrypted of Lena histogram, (g) is encrypted of Rice histogram, (h) encrypted of Peppers histogram, (i) encrypted of Cameraman histogram, and (j) encrypted of Baboon histogram

4. CONCLUSION

In this study, the combination of the SLM, Hill cipher, and Kronecker's product method in image encryption has yielded distinct outcomes across various image datasets. Among the tested images (Lena, Rice, Peppers, Cameraman, and Baboon), the encryption process resulted in the best MSE and PSNR for the Lena image, with MSE at 92.81 and PSNR at 19.43, indicating a higher level of fidelity and quality. Furthermore, the encryption of 64×64-pixel images demonstrated consistently high values for NPCR and

UACI, affirming the robustness of the encryption process against key modifications. The highest NPCR and UACI values were consistently achieved for the Cameraman image, denoting notable alterations in pixel values and enhanced unpredictability. When considering 128×128-pixel images, the encryption performance, measured by NPCR and UACI, remained commendable across the tested images. The encryption scheme involving SLM, Hill cipher, and Kronecker's product has exhibited its effectiveness in balancing security and perceptual quality, with the Lena image consistently demonstrating superior performance based on MSE, PSNR, NPCR, and UACI metrics. Our findings align with recent observations indicating the effectiveness of combining different encryption techniques in achieving a balance between security and perceptual quality in image encryption. Specifically, the integration of SLM, Hill cipher, and Kronecker's product method has demonstrated superior performance across various image datasets, with the Lena image consistently exhibiting the highest fidelity and quality metrics such as MSE and PSNR. This further corroborates existing research suggesting that the choice of encryption methods significantly influences the overall encryption performance, emphasizing the importance of selecting appropriate algorithms to ensure both robust security and minimal degradation in image quality. Future research endeavors in the realm of image encryption could explore advanced hybrid encryption techniques by integrating emerging cryptographic algorithms and artificial intelligence-based methodologies. Incorporating deep learning models, such as neural networks, could potentially enhance encryption processes by learning intricate patterns within images and adapting encryption strategies accordingly. Additionally, investigating the applicability of quantum computing in image encryption may open new frontiers, given its potential to revolutionize cryptographic methods. The exploration of lightweight encryption algorithms designed for resource-constrained devices could also be a promising avenue for research, catering to the growing demands of secure image communication in diverse technological environments. Furthermore, considering the increasing prevalence of multimedia data, future studies may focus on developing encryption techniques specifically tailored for various types of multimedia content beyond static images, including videos and 3D models.

ACKNOWLEDGEMENTS

Thanks to the Research Center for Intelligent Distributed Surveillance and Security, Dian Nuswantoro University, Semarang, which has supported this research.

FUNDING INFORMATION

This research was funded by the Research Center for Intelligent Distributed Surveillance and Security, Dian Nuswantoro University, Semarang in accordance with Decree No. 023/LL6/PgB/AL.04/2024 and 061/A.38-04/UDN-09/VI/2024.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Heru Lestiawan	✓	✓	✓	✓	✓	✓		✓	✓	✓		✓	✓	✓
Ramadhan Rakhmat Sani	✓	✓	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓
Abdussalam	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓			✓
Eko Hari	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓		
Rachmawanto														
Purwanto	✓	✓		✓	✓	✓		✓	✓	✓				
Christy Atika Sari	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓		
Mohamed Doheir	✓	✓		✓	✓	✓		✓	✓	✓			✓	

- C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis
- I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing
- Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

INFORMED CONSENT

We have obtained informed consent from all individuals included in this study.

ETHICAL APPROVAL

The research related to human use has been complied with all the relevant national regulations and institutional policies in accordance with the tenets of the Helsinki Declaration and has been approved by the authors' institutional review board or equivalent committee

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.




REFERENCES

- [1] K. N. Madhusudhan and P. Sakthivel, "A secure medical image transmission algorithm based on binary bits and Arnold map," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 5, pp. 5413–5420, May. 2021, doi: 10.1007/s12652-020-02028-5.
- [2] S. Patel, B. K. P., and R. K. M., "Symmetric keys image encryption and decryption using 3D chaotic maps with DNA encoding technique," *Multimedia Tools and Applications*, vol. 79, no. 43–44, pp. 31739–31757, Nov. 2020, doi: 10.1007/s11042-020-09551-9.
- [3] M. Roy, S. Chakraborty, and K. Mali, "An optimized image encryption framework with chaos theory and EMO approach," *Multimedia Tools and Applications*, vol. 82, no. 20, pp. 30309–30343, Aug. 2023, doi: 10.1007/s11042-023-14438-6.
- [4] C. L. Chowdhary, P. V. Patel, K. J. Kathrotia, M. Attique, P. Kumaresan, and M. F. Ijaz, "Analytical study of hybrid techniques for image encryption and decryption," *Sensors (Switzerland)*, vol. 20, no. 18, pp. 1–19, 2020, doi: 10.3390/s20185162.
- [5] M. Gabr, Y. Korayem, Y.-L. Chen, P. L. Yee, C. S. Ku, and W. Alexan, " R^3 —Rescale, Rotate, and Randomize: A Novel Image Cryptosystem Utilizing Chaotic and Hyper-Chaotic Systems," *IEEE Access*, vol. 11, pp. 119284–119312, 2023, doi: 10.1109/ACCESS.2023.3326848.
- [6] A. Tripathi and J. Prakash, "A blockchain enabled reversible data hiding based on image smoothing and interpolation," *Multimedia Tools and Applications*, Sep. 2023, doi: 10.1007/s11042-023-16695-x.
- [7] N. Abohamra, S. A. Salheen, and A. A. Ahmed, "Hide Text within Image Watermarks by Employing the Least Significant Bit (LSB) Technique for Enhanced Data Security," *The North African Journal of Scientific Publishing (NAJSP)*, vol. 1, no. 4, pp. 54–60.
- [8] R. Zahid *et al.*, "Secure Data Management Life Cycle for Government Big-Data Ecosystem: Design and Development Perspective," *Systems*, vol. 11, no. 8, pp. 1–18, Jul. 2023, doi: 10.3390/systems11080380.
- [9] E. J. G. H. M. A. and F. H. M. S., "Enhanced Security: Implementation of Hybrid Image Steganography Technique using Low-Contrast LSB and AES-CBC Cryptography," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 8, pp. 1–8, 2022, doi: 10.14569/IJACSA.2022.01308104.
- [10] M. S. Abdalzaher, M. M. Fouda, and M. I. Ibrahim, "Data Privacy Preservation and Security in Smart Metering Systems," *Energies*, vol. 15, no. 19, Oct. 01, 2022, doi: 10.3390/en15197419.
- [11] M. M. Ogonji, G. Okeyo, and J. M. Wafula, "A Survey on Privacy and Security of Internet of Things," *Computer Science Review*, vol. 38, 2020, doi: 10.1016/j.cosrev.2020.100312.
- [12] P. N. Lone, D. Singh, V. Stoffová, D. C. Mishra, U. H. Mir, and N. Kumar, "Cryptanalysis and Improved Image Encryption Scheme Using Elliptic Curve and Affine Hill Cipher," *Mathematics*, vol. 10, no. 20, Oct. 2022, doi: 10.3390/math10203878.
- [13] V. Sathananthavathi, K. Ganesh Kumar, and M. Sathish Kumar, "Secure visual communication with advanced cryptographic and image processing techniques," *Multimedia Tools and Applications*, 2023, doi: 10.1007/s11042-023-17224-6.
- [14] M. Kaur, S. Singh, and M. Kaur, "Computational Image Encryption Techniques: A Comprehensive Review," *Mathematical Problems in Engineering*, vol. 2021, 2021, doi: 10.1155/2021/5012496.
- [15] R. Denis and P. Madhubala, "Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems," *Multimedia Tools and Applications*, vol. 80, no. 14, pp. 21165–21202, Jun. 2021, doi: 10.1007/s11042-021-10723-4.
- [16] H. Alloui and Y. Mourdi, "Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive Survey," *Sensors*, vol. 23, no. 19, Oct. 01, 2023, doi: 10.3390/s23198015.
- [17] T. Zhang and Y. Ma, "Stable Image Encryption Algorithm Based on Expanded One-dimensional Chaotic Jumping and Parallel Encoding Operation Grouping," *IEEE Access*, pp. 108746–108760, Sep. 2023, doi: 10.1109/access.2023.3312611.
- [18] D. E. Mfungo, X. Fu, X. Wang, and Y. Xian, "Enhancing Image Encryption with the Kronecker xor Product, the Hill Cipher, and the Sigmoid Logistic Map," *Applied Sciences (Switzerland)*, vol. 13, no. 6, Mar. 2023, doi: 10.3390/app13064034.
- [19] D. E. Mfungo, X. Fu, Y. Xian, and X. Wang, "A Novel Image Encryption Scheme Using Chaotic Maps and Fuzzy Numbers for Secure Transmission of Information," *Applied Sciences (Switzerland)*, vol. 13, no. 12, Jun. 2023, doi: 10.3390/app13127113.
- [20] D. E. Mfungo and X. Fu, "Fractal-Based Hybrid Cryptosystem: Enhancing Image Encryption with RSA, Homomorphic Encryption, and Chaotic Maps," *Entropy*, vol. 25, no. 11, pp. 1–29, Oct. 2023, doi: 10.3390/e25111478.
- [21] H. Yi, "Improving cloud storage and privacy security for digital twin based medical records," *Journal of Cloud Computing*, vol. 12, no. 1, Dec. 2023, doi: 10.1186/s13677-023-00523-6.
- [22] N. Gupta and R. Vijay, "Hybrid image compression-encryption scheme based on multilayer stacked autoencoder and logistic map," *China Communications*, vol. 19, no. 1, pp. 238–252, 2022, doi: 10.23919/JCC.2022.01.017.




- [23] M. D. Gietaneh and T. B. Akele, "Enhancing the Hill Cipher Algorithm and Employing a One Time Pad Key Generation Technique," *Abyssinia Journal of Engineering and Computing*, vol. 3, no. 1, pp. 1–10, 2023.
- [24] X. Zhu, H. Liu, Y. Liang, and J. Wu, "Image encryption based on Kronecker product over finite fields and DNA operation," *Optik (Stuttg)*, vol. 224, 2020, doi: 10.1016/j.ijleo.2020.164725.
- [25] P. Ramasamy, V. Ranganathan, S. Kadry, R. Damaševičius, and T. Blažauskas, "An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using Enhanced Logistic-Tent Map," *Entropy*, vol. 21, no. 7, Jul. 2019, doi: 10.3390/e21070656.
- [26] C.-L. Li, Y. Zhou, H.-M. Li, W. Feng, and J.-R. Du, "Image encryption scheme with bit-level scrambling and multiplication diffusion," *Multimedia Tools and Applications*, vol. 80, no. 12, pp. 18479–18501, 2021, doi: 10.1007/s11042-021-10631-7.
- [27] M. Arora and M. Khurana, "Secure image encryption technique based on jigsaw transform and chaotic scrambling using digital image watermarking," *Optical and Quantum Electronics*, vol. 52, no. 2, pp. 1–30, 2020, doi: 10.1007/s11082-019-2130-3.
- [28] J. Wang *et al.*, "A Novel Underwater Acoustic Signal Denoising Algorithm for Gaussian/Non-Gaussian Impulsive Noise," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 429–445, Jan. 2021, doi: 10.1109/TVT.2020.3044994.
- [29] A. Shafique, J. Ahmed, M. U. Rehman, and M. M. Hazzazi, "Noise-Resistant Image Encryption Scheme for Medical Images in the Chaos and Wavelet Domain," *IEEE Access*, vol. 9, pp. 59108–59130, 2021, doi: 10.1109/ACCESS.2021.3071535.
- [30] C. A. Sari, M. H. Dzaki, E. H. Rachmawanto, R. R. Ali, and M. Doheir, "High PSNR Using Fibonacci Sequences in Classical Cryptography and Steganography Using LSB," *International Journal of Intelligent Engineering and Systems*, vol. 16, no. 4, pp. 568–580, 2023, doi: 10.22266/ijies2023.0831.46.
- [31] Y. Alghamdi, A. Munir, and J. Ahmad, "A Lightweight Image Encryption Algorithm Based on Chaotic Map and Random Substitution," *Entropy*, vol. 24, no. 10, Oct. 2022, doi: 10.3390/e24101344.
- [32] S. Dua, J. Singh, and H. Parthasarathy, "Image forgery detection based on statistical features of block DCT coefficients," in *Procedia Computer Science*, Elsevier B.V., 2020, pp. 369–378, doi: 10.1016/j.procs.2020.04.038.
- [33] T. Khanam, P. K. Dhar, S. Kowsar, and J. M. Kim, "SVD-based image watermarking using the fast Walsh-Hadamard transform, key mapping, and coefficient ordering for ownership protection," *Symmetry (Basel)*, vol. 12, no. 1, Jan. 2020, doi: 10.3390/SYM12010052.
- [34] U. Sara, M. Akter, and M. S. Uddin, "Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study," *Journal of Computer and Communications*, vol. 07, no. 03, pp. 8–18, 2019, doi: 10.4236/jcc.2019.73002.

BIOGRAPHIES OF AUTHORS






Heru Lestiawan    received a bachelor's degree in informatics management from STIMIK Dian Nuswantoro in 1996 and received a master's degree in informatics engineering from the Universitas Dian Nuswantoro in 2004. He has been a lecturer since 1996 and has developed several Intellectual Property research results. He is currently actively teaching and writing scientific articles. The research he is pursuing is image processing, image analysis, data hiding, and watermarking. He can be contacted at email: heru.lestiawan@dsn.dinus.ac.id.






Ramadhan Rakhmat Sani    received a bachelor's degree in Informatics Engineering from the Universitas Dian Nuswantoro in 2011 and received a double master's degree from the University of Dian Nuswantoro and University Teknikal Malaysia Melaka (UTeM) in 2014. Currently serving as a coordinator in the field of data security studies since 2023. The research topic pursued is data security. He can be contacted at email: ramadhan_rs@dsn.dinus.ac.id.






Abdussalam    received bachelor's and master's degrees from the Universitas Dian Nuswantoro respectively in 2007 and 2015. Becoming a lecturer in 2002 served as Head of the Hardware, Software, and Network Division of the Computer Laboratory, Faculty of Computer Science, Universitas Dian Nuswantoro. His research areas of interest are security data and computer networks. He can be contacted at email: grey.salam@dsn.dinus.ac.id.






Eko Hari Rachmawanto    received a Bachelor's degree at the Department of Informatics Engineering Universitas Dian Nuswantoro, Semarang, Indonesia, in 2009 and a dual Master's degree in the Department of Informatics Engineering, Universitas Dian Nuswantoro, Semarang, Indonesia and in Faculty of Computer Science and Information, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia, in 2012. He is currently the lecturer and researcher at the Faculty of Computer Science, Universitas Dian Nuswantoro, Semarang, Indonesia. He has authored or co-authored more than 100 refereed journal and conference papers. He is also a reviewer of more than 10 Scopus-indexed journals indexed by Scopus. His research interests include image processing, especially data hiding, cryptography, image processing, machine learning, and deep learning. He can be contacted at email: eko.hari@dsn.dinus.ac.id.






Purwanto    is currently an Associate Professor in the Faculty of Computer Science at the Universitas Dian Nuswantoro, Semarang, Indonesia. He received his Ph.D. degree from the Faculty of Computing and Informatics Multimedia University, Cyberjaya, Malaysia. Now, he serves as Head of the Master's Degree Program at the Universitas Dian Nuswantoro. He has published research papers in reputed international journals and conferences. His current research interests image processing, machine learning, and deep learning. He can be contacted at email: purwanto@dsn.dinus.ac.id.



Christy Atika Sari    received the master in Informatic Engineering from Universitas Dian Nuswantoro and University Teknikal Malaysia Melaka (UTeM) in 2012. She is currently active as author in international journal and conference Scopus indexed. She also awarded as best author and best paper in national and international conference in 2019 and 2020 respectively and awarded from Ristekbrin DIKTI as the Indonesian top 50 best researchers in 2020. She currently as lecturer in intelligent systems and continue to develop the research field image processing, deep learning, and data hiding. She can be contacted at email: christy.atika.sari@dsn.dinus.ac.id.



Mohamed Doheir    received his doctorate in Healthcare Management in 2020 from the University Teknikal Malaysia Melaka (UTeM). He received his master's from the University Teknikal Malaysia Melaka (UTeM) in 2012. His current research such as cloud computing, information technology, and system management. Since 2022, he served as dean of the Faculty of Technopreneurship, the University Teknikal Malaysia Melaka, Malaysia. He can be contacted at email: doheir@utem.edu.my.